Securing the eCampus 2013
Building a Culture of Information Security in an Academic Institution
July 16-17, 2013

Agenda

Tuesday, 16 July
Kemeny Hall, Bradley Lecture Hall, Room 008

8:30AM Conference Registration and Continental Breakfast
Location: Haldeman Center, Russo Gallery

9:00AM Welcoming Remarks
Ellen Waite-Franzen
Vice President for Information Technology and Chief Information Officer, Dartmouth
Location: Kemeny Hall, Bradley Lecture Hall, Room 008

9:10AM Criticality, Rejectionists, Risk Tolerance
Dan Geer
CISO, In-Q-Tel

10:05AM The Three Lost Battles: Winning the War on Cybercrime
George Tubin
Senior Security Strategist, Trusteer

11:00AM Break

11:30AM Understanding Cybersecurity Policy from a Risk Management Lens
Rodney Petersen
Managing Director of the Washington Office and Senior Government Relations Officer at EDUCAUSE

12:10PM Lunch
Location: Fahey Lounge
Birds of a Feather Topic Tables
2:00PM  Risk-Based Cyber Security for the 21st Century  
*Ron Ross*  
Fellow, National Institute of Standards and Technology (NIST)

2:30-5:30PM  Vendor Room Open  
**Location:** Haldeman Center, Room 031

2:55PM  Privacy, Security, and Compliance: Strange Bedfellows, or Marriage Made in Heaven?  
*Michael Corn*  
Chief Privacy and Security Officer, University of Illinois Urbana-Champaign

3:50PM  Break  
Refreshments available in Haldeman Center, Room 031

4:10PM  The Millennial Cybersecurity Project: Improving Awareness of and Modifying Risky Behavior in Cyberspace  
*Noel Greis*  
Director, Center for Logistics and Digital Strategy Kenan-Flagler Business School, University of North Carolina at Chapel Hill

5:05PM  Wrap-up  
*Tom Candon*  
Institute for Security, Technology, and Society, Dartmouth

5:30PM  Social  
*Sponsored by Cisco Systems and Presidio*  
**Location:** Paganucci Lounge, Class of '53 Commons

7:00PM  Free time for dinner
Wednesday, 17 July
Haldeman Center

8:30AM  Continental Breakfast
Location: Haldeman Center, Room 031

8:30AM – 12:30PM  Vendor Room Open

9:00AM  Day 2 Kick-off
Location: Haldeman Center, Kreindler Auditorium, Room 041

9:15AM  Break-out Session 1

The IAM Program Development Toolkit
David Sherry
Chief Information Security Officer, Brown University
Location: Haldeman Center, Room 124

Multi-factor Authentication
Richard Biever, Chief Information Security Officer, Duke University
Shilen Patel, Senior IT Analyst, Duke University
Adam Goldstein, IT Security Engineer, Dartmouth
Sean McNamara, Software Engineer, Dartmouth
Location: Haldeman Center, Room 125

Panel Discussion on K-12 Security Awareness
Moderated by: Emily Eckland, Director of Digital Strategy & Awareness Campaigns, National Cyber Security Alliance
Panelists: Ellen Young, Director of IT Support, Dartmouth and Harry Vann, Network Administrator, St. Johnsbury Academy
Location: Haldeman Center, Kreindler Auditorium, Room 041
10:15AM **Break-out Session 2**

*Richard Biever*, Chief Information Security Officer, Duke University  
*Shilen Patel*, Senior IT Analyst, Duke University  
*Adam Goldstein*, IT Security Engineer, Dartmouth  
*Sean McNamara*, Software Engineer, Dartmouth  
**Location**: Haldeman Center, Room 125

**Panel Discussion on K-12 Security Awareness**  
**Moderated by**: *Emily Eckland*, Director of Digital Strategy & Awareness Campaigns, National Cyber Security Alliance  
**Panelists**: *Ellen Young*, Director of IT Support, Dartmouth and *Harry Vann*, Network Administrator, St. Johnsbury Academy  
**Location**: Haldeman Center, Kreindler Auditorium, Room 041

---

**Misperception and Security**  
*Sean Smith*  
Professor of Computer Science, Dartmouth  
**Location**: Haldeman Center, Room 124

11:15AM **Break-out Session 3**

**The IAM Program Development Toolkit**  
*David Sherry*  
Chief Information Security Officer, Brown University  
**Location**: Haldeman Center, Room 125

**Misperception and Security**  
*Sean Smith*  
Professor of Computer Science, Dartmouth  
**Location**: Haldeman Center, Room 124

12:30PM **Lunch**  
**Location**: Dartmouth Outing Club (DOC) House on Occom Pond  
*Bus service will be provided from the Haldeman Center to the DOC House.*

1:15PM **Five Minutes to Security**

1:20PM **Conference Wrap-up**  
*Steve Nyman*  
Chief Information Security Officer, Dartmouth College

2:00PM **Conference Concludes**
Criticality, Rejectionists, Risk Tolerance – Dan Geer
Risk is a consequence of dependence. Because of the shared dependence, aggregate societal dependence on the Internet is not estimable. If dependencies are not estimable, they will be underestimated. If they are underestimated, they will not be made secure over the long run, only over the short. As risks become increasingly unlikely to appear, the interval between events will grow longer. As the latency between events grows, the assumption that safety has been achieved will also grow, thus fueling increased dependence in what is now a positive feedback loop.

The Three Lost Battles: Winning the War on Cybercrime – George Tubin
Cybercriminals take advantage of ongoing application vulnerabilities and social engineering to install advanced malware on consumer devices as well as employee devices used to access corporate networks. Advanced malware effectively bypasses authentication technologies and evades anti-virus software applications. Although several key malware defenses have been bypassed, effective cybercrime prevention approaches do exist to help win the war on cybercrime. This session will provide an overview of:

- The methods cybercriminals use to successfully install advanced malware on endpoint devices
- The most recent fraud techniques uncovered by Trusteer research over the past several months
- The evolving risks due to cybercrime, including: attacks on employee devices, implications of recent US court rulings on bank fraud liability
- Best practices and practical solutions to mitigate the increased risk of fraud from both customer and employee devices

Understanding Cybersecurity Policy from a Risk Management Lens – Rodney Petersen
As governments seek to establish the right legal frameworks and gain political support for the means to secure critical infrastructures, organizations must continue to establish and execute an information security program that is designed to safeguard institutional cyber assets. Risk management is the process by which an institution manages the strategic, operational, financial, legal, and reputational impact of cyber events. This presentation will provide an update on public policy initiatives in Washington and the implications for colleges and universities who are striving to create a risk-aware culture at their institution.

Risk-Based Cyber Security for the 21st Century – Ron Ross
Cyber attacks on information systems today are often aggressive, disciplined, well-organized, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or grave damage to the national and economic security interests of the United States. Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks. NIST in partnership with the Department of Defense (DoD), the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common information security framework for the federal government, contractors, and organizations in the private sector choosing to use the framework on a voluntary basis. The intent of the common framework is to improve information security and to strengthen risk management processes. The six-step Risk Management Framework (RMF), the central construct of the common framework, emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems. The RMF changes the
traditional focus of cybersecurity as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.

Privacy, Security, and Compliance: Strange Bedfellows, or a Marriage Made in Heaven? – Michael Corn
Where does privacy belong in the college/university ecosystem, and what should its relationship be with security and compliance? Are the three areas best kept separate and distinct? Should there be some overlap? Or would a single office, officer, and/or reporting line enable a big picture of the whole? This session examines several of the campus issues lying at the intersection of privacy, security, and compliance and provides some insight for institutional leaders as they plan strategic directions.

The Millennial Cybersecurity Project: Improving Awareness of and Modifying Risky Behavior in Cyberspace – Noel Greis
The Millennial Cybersecurity Project offers critical insights into millennial behaviors that can inform policies for building awareness of and modifying risky behavior in cyberspace—especially with respect to password and phishing behavior. While the popular press tends to categorize millennials as the always "connected" generation, there are considerable differences in awareness of safe cybersecurity practices and the attendant risks. The project observed different types of behaviors that reflect a balance between awareness of cybersecurity best practices and the risk profile of the student. For those with lower awareness of policies and safe practices, technology-mediated messaging and interventions can be effective in reducing risky behavior. While we were unable to discern key differences in the effectiveness of different types of intervention, our results suggest that a combination of the right "messaging" that encodes a strategy in a format that millennials are used to (i.e. short, visual and colorful), delivery of that message by some form of self-representation or avatar, or online feedback about risky behavior in real-time could be effective at reducing risky behaviors.

Day 2, July 17th

The IAM Program Development Toolkit: An EDUCAUSE Resource – David Sherry
Throughout 2012 and early 2013, a team of higher education practitioners from across the country developed an Identity and Access Management Toolkit at the request of EDUCAUSE. This session will review the final product, and is meant to be a discussion and information sharing session for those who attend. It is led by a member of the working group, who will share the methodology and facilitate discussion on its use as a resource for those institutions which are just starting a program, or benchmarking a current program.

Misperception and Security – Sean Smith
Computer security aims to ensure only "good" behavior happens in computer systems, despite potential action by malicious adversaries. Consequently, the field has focused primarily on the technology to prohibit "bad things," according to some set of rules, and to a lesser extent on the structure of such rules.

Unfortunately, fieldwork and anecdotes report how we keep getting the rules "wrong."

Interestingly, the computer security field has largely ignored the process by which humans produce these sets of rules. However, psychology and related disciplines can tell us a lot about such processes—including ways the human mind systematically misperceives things when making evaluations and judgments. In this talk, we will examine whether systematic flaws in how humans produce these rule sets lie at the core of real-world security frustration—and whether we can use these insights to improve the situation. The talk will draw on IT security issues in real-world domains including finance, healthcare, power.